Cybersecurity

and Safeguarding Electronic Transactions in the Pacific Islands

Policy Brief

OCTOBER 2019

ADB Australian Aid European Union JICA NEW ZEALAND Aid Programme WORLD BANK GROUP

This report is published by the Pacific Region Infrastructure Facility (PRIF), a multi-development partner coordination, research and technical assistance facility that supports infrastructure development in the Pacific. PRIF member agencies: Asian Development Bank (ADB), Australian Department of Foreign Affairs and Trade (DFAT), European Investment Bank (EIB), European Union (EU), Japan International Cooperation Agency (JICA), New Zealand Ministry of Foreign Affairs and Trade (NZMFAT), United States Department of State (USDoS) and the World Bank (WB).

The PRIF would like to thank the governments of all participating countries for their extensive inputs, without which this study would not have been possible. We also wish to thank the authors, Chapman Tripp in association with Deloitte and Solutions Consulting House, who worked under the supervision of Michel Dorval, Technical manager of the facility, and the PRIF agencies experts who kindly provided guidance during the study.

PRIF Coordination Office, c/- Asian Development Bank
Level 20, 45 Clarence Street, Sydney, New South Wales, Australia, 2000
Tel: +61 2 8270 9444 Email: enquiries@theprif.org Website: www.theprif.org

Acronyms and Definitions

AFP	Australian Federal Police, Australia
APNIC	Asia-Pacific Network Information Centre
Budapest Convention	Council of Europe Convention on Cybercrime, CETS No 185
ccTLD	Country Code Top-Level Domain
CERT	Computer Emergency Response Team (also known as a CSIRT, a Computer Security Incident Response Team)
Convention on the Rights of the Child	United Nations Convention on the Rights of the Child, UNTS 1577
CTO	Commonwealth Telecommunications Organisation
Cyber Safety Pasifika	A cyber awareness-raising programme developed by the AFP, working with the PICP
DFAT	Department of Foreign Affairs and Trade, Australia
FBI	Federal Bureau of Investigation, United States
ICANN	Internet Corporation for Assigned Names and Numbers
ICB4PAC	Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries, a project undertaken in 2013 by the ITU, in association with PIFS, SPC, PITA, PIRRC and USP
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organisation
ITU	International Telecommunication Union
ITU-IMPACT Initiative	International Multilateral Partnership Against Cyber Threats, a partner of the ITU
Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography	United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, UNTS 2171
PacCERT	Pacific Computer Emergency Response Team, previously headquartered at USP (and now defunct)
PaCSON	Pacific Cyber Security Operational Network
PICP	Pacific Islands Chiefs of Police
PICISOC	Pacific Islands Chapter of the Internet Society
PIFS	Pacific Islands Forum Secretariat

PILON	Pacific Islands Law Officers' Network
PIRRC	Pacific ICT Regulatory Resource Centre, funded under the World Bank's Pacific Regional ICT Regulatory Development Project
PITA	Pacific Islands Telecommunications Association
PRIF	Pacific Region Infrastructure Facility
PTCCC	Pacific Transnational Crime Coordination Centre, an institution of the PTCN
PTCN	Pacific Transnational Crime Network, an initiative of the PICP
SFO	Serious Fraud Office, New Zealand
SPC	Secretariat of the Pacific Community
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
Uniform Domain Name Dispute Resolution Procedure	A process for the resolution of internet domain name registration disputes, created by ICANN
USP	University of the South Pacific

Table of Contents

Cybercrime is becoming a greater risk when doing business in Asia-Pacific (APAC) as compared to North America and Europe. Rapidly growing connectivity and the accelerating pace of digital transformation expose the APAC region, and make it particularly vulnerable to cyber exploitation.

- Marsh & McLennan Companies, “Cyber Risk in Asia-Pacific”

Introduction

Context

The Pacific Region Infrastructure Facility has identified a critical need to assess the environment for cybersecurity and electronic transactions across the Pacific region, and develop an action plan.

Governments and development partners across the Pacific have been investing in telecommunications and ICT reforms and infrastructure. To maximise the benefit of these reforms and the new infrastructure, national legal and regulatory frameworks should promote confidence and trust in a broadband-enabled, digital economy.

The Pacific Region Infrastructure Facility has engaged Chapman Tripp, together with Deloitte and Solutions Consulting House, to consider the legal and regulatory frameworks supporting cybersecurity and e-transactions in the Pacific, identify potential gaps, and recommend possible reforms in participating countries.[1] We have also undertaken a regional cyber risk assessment, led by Deloitte, for the purpose of understanding the current and potential impact of cyber incidents in the Pacific and prioritising initiatives to mitigate these risks.

We intend the Cyber Risk Assessment and the Policy and Legal Gap Analysis to inform discussions within and between participating countries, donor agencies, and other stakeholders on the development of cyber and electronic transaction frameworks. This Policy Brief is a summary extract of the main report which is available at www.theprif.org.

[1] The participating countries are Cook Islands, FSM, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Palau, PNG, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.

Cyber Risk Assessment

Executive Summary

Background and Introduction

This Cybersecurity Assessment document provides a view of the key cyber risks for the Pacific Island regions and the 14 countries of the study which include Cook Islands, Fiji, FSM, Kiribati, Marshall Islands, Nauru, Niue, Palau, PNG, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.

Approach

In summary, the cyber risk assessment and the regional recommendations have been developed through a combination of:

- Seven in-country visits during April 2018 – July 2019
- A regional workshop
- Desk-based research

Key Insights

We have identified a number of relevant insights that will be important as a means to framing up effective recommendations and action plans. A few key ones are set out below (further detail is provided below under "Detailed Insights"):

1. **The cyber risk is real and growing, and the current need to address this risk is critical.**
   The Pacific Region is highly exposed to a range of cyber threats, spanning from email fraud, ransomware and card skimming to cyber bullying and child pornography. This has already affected countries both financially (impacts and losses from cyber crime stretch into the millions of US dollars) and has caused harm to the physical and mental well-being of citizens. This risk is growing rapidly with greater connectivity and more systems and information being moved online.
2. **Financial losses through fraud/scams, and the protection of children from cyber bullying and exploitation are the highest current realised cyber risks for the region.**
   We were informed of numerous cases of significant cyber fraud involving government and business email compromise or imitation, and the subsequent creation of fake payments/invoices. The cyber fraud events we were informed of totalled into the millions of US dollar, including some single events of US$300,000 or higher. In addition, cyber bullying was noted by many Pacific stakeholders as the highest existing cyber risk – in particular – severe bullying, revenge porn and objectionable materials posted on social media.

3. **There is a low level of cyber security maturity across the region.**
   The rise in cyber security risk for the region is relatively recent on a global scale. This is due to the rapid increase in connectivity and use of online services that has been stimulated by the installation of fibre-optic broadband submarine cables for a number of participating countries. Building awareness at a senior level and creating a country-level mandate (with the appropriate regional level support and initiatives) to uplift cyber security will be critical to enabling participating countries to take advantage of the social and economic benefits of being connected. This maturity gap needs to be addressed to reduce losses and harm as a high priority.

4. **Any initiatives in the region should be linked up with existing workstreams and focus on local ownership, bilateral opportunities and building local capability.**
   There have been a number of initiatives targeted at uplifting cyber security in the Pacific, however a number of these initiatives have failed or had a restricted impact. Traditionally, the approach has not been linked up between various donor agencies, regional governments and partners. Specifically, we believe the following are key elements to a successful initiative for cyber security:
   - Take advantage of existing forums and initiatives, as opposed to creating overlaps with new initiatives.
   - Focus on bilateral opportunities that enable governments in the region to share technology, resources and templates.
   - Local ownership, skills development, documentation and operational funding are critical to long-term success.
   - Secondment and hands-on training are significantly more valuable than shorter (circa 1-5 day) classroom sessions.
   - Procurement of technology should be linked up across countries (to share skills), include cyber security requirements and should be driven by local needs.
   - Consider, but do not be limited by regional alignment and context.

We have identified numerous initiatives that have been or are still being supported in the region. Based on our research and the experience gained locally and internationally during these projects, a number of regional challenges have been identified and should be considered to continually improve the effectiveness of new projects and initiatives. Some of these challenges are:

- **Difficulties in achieving sustainability and ongoing support.** While there have been a number of useful initiatives undertaken in the region, we have observed a number of instances where insufficient ongoing support and investment have reduced their effectiveness. For example, the PacCERT initiative, and additionally a number of local initiatives related to new tech platforms and cyber strategies and legislation.
- **A lack of visibility and coordination of cyber-relevant programmes in place.** This has made it difficult for cyber related investment to be efficient and effective.
- **A large portion of attempts to reduce Cyber risk rely heavily on taking a pan-region approach.** It has been difficult to attract ongoing support and investment in regional investments. Stakeholders in the participating countries we met have specifically requested support for domestic initiatives and regional information sharing/co-ordination rather than larger scale regional initiatives. Notwithstanding a need to consider bilateral opportunities and pooling regional resources, incident reporting/information and training opportunities – our observation has been that each country has their own strong independent identity and cultural context and some projects will be more effective when they are executed within these local contexts.

Key Risks

The participating countries identified in the Pacific region face significant risk from a cyber attack or major incident. For the purpose of this assessment, we established and assessed the region against 14 key types of cyber risks that the Pacific Region currently faces across 4 harm areas, which are outlined in the table below.

The risks below have been rated (red for high, orange for medium and green for low) based on their potential impact and likelihood.

Economic	Facilitation of international money laundering and funding of terrorism	Financial harm due to fraud or unauthorised access to banking	Inability to process or receive international payments	Inability to meet international standards for e-transactions (i.e. PCI)	
Safety and Wellbeing	Facilitation of the creation, transmission or sale of objectionable or pirated material (i.e. child exploitation)	Harm to individuals due to identity theft, cyber bullying or blackmail			
Disruption	Business disruption and/or impact to wellbeing due to critical infrastructure outage	Inability to facilitate secure and reliable communications channel for international relations/business	Destruction or ransom of information	Malicious altering or defacement of Government information	Interruption to logistics/travel
Trust and Reputation	Facilitation of global cyber attacks originating from the Pacific	Theft of intellectual property, personal information or sensitive data	Driving a malicious political agenda through hacktivism or social media.		

Key Current Regional Initiatives

While there are a large number of regional and local initiatives that involve positive cyber security outcomes, we have outlined a number of initiatives below that we have observed to be effective, well received and sustainable in the medium term.

- **Australian Cyber Cooperation Program** – established in 2016, the program aims to "promote a peaceful and stable online environment and improve cyber resilience". Australia has increased funding for the program from $4m (2016) to $38m (to 2022) and New Zealand has committed to add further support. The program has 5 areas of focus:
    1. **International cyber stability framework:** promoting an understanding of how existing international law, norms and confidence building measures apply in cyberspace.
    2. **Cyber crime prevention, prosecution and cooperation:** strengthening legislative frameworks and institutional capacity to prevent, investigate and prosecute cyber crime.
    3. **Cyber incident response:** working with partners to establish and strengthen national and regional cyber incident response capability and coordinate and share cyber security threat information across the region.
    4. **Best practice technology for development:** advocating for best practice use of technology for development by integrating cyber security by design and respect for human rights online.
    5. **Human rights and democracy online:** advocating and protecting human rights and democracy online, including freedom of expression online.

Aside from supporting PaCSON (see below), Australia have supported PNG in establishing their local CERT and National Cyber Security Centre through this program.

- **Pacific Cyber Security Operational Network (PaCSON) –** funded by DFAT's Cyber Cooperation Program (see above) and initially chaired by CERT New Zealand (established April 2018), PaCSON is a network of CERTs from 14 Pacific nations. PaCSON has been established to promote sharing and collaboration in regards to cyber incident response techniques and tooling, alongside being an open forum to discuss wider cyber security concerns. PaCSON has been well-attended and is seen as an important forum in many Pacific countries, however, initial feedback suggests that it will need to be bolstered or supported by hands-on training, MOUs to support open sharing of information, and more tangible support and outputs. We have proposed a linkage between a Regional Cyber Hub and the existing PaCSON initiative within our recommendations.

- **Cyber Safety Pasifika –** this program, led by the Australian Federal Police (AFP), focuses on awareness and baseline training for the wider community, in how to stay safe online. This was the most well-known program of work relating to cyber security in the region. In particular, the AFP trained a number of Pacific-based police officers and teachers to provide cyber outreach and awareness training to their local schools and communities.

- **Pacific Islands Law Officers Network (PILON)** – this forum is helping to build awareness, skills and information sharing for the police, legal community and judiciary in regards to cyber crime. We attended the PILON regional forum in Tonga (2018) as a means of regional outreach and information gathering, which had cyber crime as the focus.

- **Council of Europe and Australian Attorney General's Office –** have both provided legislation drafting assistance and advice to a number of participating countries in the Pacific in regards to cyber crime.

- **Pacific Islands Forum Secretariat Cyber Assessment** – the Pacific Islands Forum Secretariat performed an assessment on the current state and risk in regards to cyber security – which identified the following key areas of focus:
    - promoting and supporting Forum Members accession to the Budapest Convention;
    - sharing information on cybersecurity and cyber crime threats and trends;
    - supporting the development of national cyber policies and legislation;
    - promoting awareness and educating our people on responsible cyber behaviour; and,
    - development and strengthening of Computer Emergency Response Team (CERT) capacities (national and regional).

Proposed Action Plan

We have outlined country-specific recommendations within the full Cyber Risk Assessment report. To support the Pacific Region to better respond to the cyber risks identified through our analysis, there are 7 key regional recommendations that will have a significant impact on mitigating cyber risk across the region:

Activity	Priority	Investment Level
1. Cyber Governance and Strategy Model **Issue:** Difficulties identifying and engaging with local representatives, alongside varying approaches to the governance of Cyber. **Solution:** A consistent set of key roles and a high-level operating model and strategy template/guidance should be developed for Cyber in each country within the region, alongside appropriate briefing pack/s with relevant information for senior Government officials.	**High**	**Medium**

Activity	Priority	Investment Level
2. Pacific Regional Cyber Hub **Issue:** Disparate sources of information on Cyber and related activities, alongside an immediate need for advanced technical capability and hands-on training for the region. **Solution:** Linking to and building upon the successful baseline established by the PaCSON forum for cyber security, the Regional Hub should be an iterative project to consolidate knowledge, training and capability. While initially a website would be beneficial to provide a single portal for Cyber in the region, a physical, staffed entity which owns templates and guidance, provides advanced cyber response support, performs vulnerability testing, and most importantly offers secondment opportunities for local cyber professionals to build their skillset. The Regional Hub should also provide a response capability for online child safety concerns (i.e. linkages to social media for removing offensive content).	**High**	**High**
3. Cyber Crime Legislation and Enforcement Capability Building **Issue:** Insufficient capability within law enforcement and judiciary to support cyber crime investigation and prosecution, alongside a lack of fit-for-purpose legislation. **Solution:** Targeted and ongoing awareness building and training for the enforcement, investigation and legal response to cyber crime throughout the region.	**High**	**Medium**
4. Uplift National CERT Capabilities **Issue:** A number of participating countries are establishing CERT capabilities but the lack of consistency in their role reduces their effectiveness and ability to share information. **Solution:** A template/model for local CERT and/or Cyber response functions, alongside financial and resource support for execution and ongoing operation.	**Medium**	**Medium**
5. Security Requirements for Critical Infrastructure **Issue:** There are a number of industrial control systems in use to manage critical infrastructure (i.e. controlling power, chemicals in the water supply and telecommunications), however international standards are not achievable and a fit-for-purpose approach for the region does not exist. **Solution:** A minimum set of security requirements and associated guidance for critical infrastructure providers which is focused on real regional risk and capability.	**Medium**	**Low**
6. Pacific Cyber Innovation Fund (Centralised Procurement) **Issue:** Donor-led projects are often executed in isolation of each other, and opportunities to leverage existing initiatives, and importantly learnings from failed/previous initiatives, are not realised. **Solution:** A platform to improve procurement outcomes and enable local and international entities to request funds for specific tactical or targeted cyber projects, including requirements for these projects.	**Low**	**High**

Detailed Insights

We have framed the following key insights through our work with a view to providing important regional context relevant to cyber risk in the region, as well as, being designed to support the successful implementation of recommendations.

The overall positive impact of connectivity to wellbeing and the economy of Pacific Island participating countries should not be understated. This is evidenced by demand – including exponential year-on-year growth of data consumption throughout the region, especially in the young generation.

This connectivity has huge benefits to individuals - enabling learning (both international and local), access to international employment opportunities, entertainment, and stronger links to family abroad. In addition, the positive social and economic impacts of this connectivity are visible – enabling international business/transactions, reliable and efficient methods for business and communication, and making local knowledge and information available to potential investors, visitors and tourists.

1. **The cyber risk to the region is real and growing, and the current need to address this risk is critical.**
   The Cyber risk to the region is real and through our work we have been privy to the types of cyber incidents that the participating countries have experienced or are currently facing. These span:
   - Financial harm - e.g. business and government email compromise and associated fraud, card skimming, unauthorised access to online banking, toll call attacks, fake online businesses targeting tourists, and scams that involve sending money overseas.
   - Disruption of system resilience - e.g. internet outages due to denial of service, data loss from ransomware, blacklisting of government services/websites due to malicious activity that is coming from them, isolated incidents of power outage due to operational (potentially non-security related) issues with industrial control systems.
   - Severe harm to the well-being of people - e.g. there have been cases of child or revenge pornography being created and/or distributed, severe cyber-bullying and harassment, Facebook account hacking, fake profiles imitating prominent figures and institutions, and defamation on social media.
   - Reputational harm – e.g. theft of private or confidential information from Government and private entities (and subsequent release).

   As a measure for relative importance, the attacks we have been informed of involving financial losses include cyber-fraud related theft totalling millions of US dollars (there have been individual fraud cases of US$300,000 – US$800,000). Based on our experience as cyber incident responders, these fraud attacks are currently becoming more frequent and advanced in their methodologies on a global and regional scale.

   Cyber criminals are not restricted by geography. Our experience has shown that attackers are most likely to perform large scale untargeted attacks against entities that have poor controls, as opposed to specific targeting of businesses that may have a high pay off. This means that immediate action to assist in managing cyber security risk is critical to participating countries in the Pacific.

   Many of these countries are improving their connectivity and pushing towards eGovernment and online payment services. For example, online transactions are increasing and for some countries, having secure payments is critical because their economies are highly reliant on international remittances and tourism. Also, critical infrastructure systems such as those used to manage and control large industrial systems (such as the power grid), that can be managed remotely over the internet, are now increasingly being targeted by malicious parties and are therefore open to significant levels of potential abuse. In

many cases, attackers are looking for "training grounds" to test malware and attack vectors before targeting more advanced entities.

Cyber risk continues to grow on a global scale – with reported and insured losses increasing year-on-year. The speed of growth for Cyber risk will be higher for the Pacific region, as connectivity increases exponentially and participating countries (with support of donor agencies) drive rapid adoption of online services and eGovernment – currently with minimal security oversight or capability.

For participating countries and local SMEs that have an interest in Cyber, the awareness of risk is focused around the individual and financial impacts. There is limited awareness of the risks to overall resilience and critical infrastructure. The Pacific region can also be seen as a "soft spot" and therefore targeted by global attackers as a target (e.g. child exploitation) or a jump off point for attacks against other countries.

Currently, there are also limited local expectations for privacy and the protection of intellectual property, however we expect this will increase quite suddenly as technologies like social media collect and use more local data. This could also cause a sudden shift in local sentiment about expectations pertaining to data protection and privacy – as seen in a number of more developed countries.

2. **Financial losses through fraud/scams, and the protection of children from cyber bullying and exploitation are the highest current realised cyber risks for the region.**
While low maturity in the region creates significant exposure to cyber harm across the board, the focus of this assessment was to identify real current risk that is having a tangible impact on countries in the region. Those real current impacts are financial, and separately to children and young people who have rapidly grown a large online presence. Some examples are:
    - Business email fraud – we identified or heard about a large number of cases, totalling millions of US dollars, where money had been extracting by attackers either breaching or imitating email addresses, and sending fake invoices for payment. In some cases these attackers would gain access to multiple accounts and approve their own transactions via email. This was prevalent in nearly every participating country, and often targeted at Government.
    - Access to online banking and credit card skimming – we identify a number of active or past cases where attackers (including foreign visitors) had installed credit card skimmers and/or used stolen credit cards on local ATMs to extract money. There were other cases where bank employees and/or attackers had gained access to local online banking accounts and extracted money.
    - Cyber bullying – many Pacific stakeholders noted this as the highest current impact in regards to cyber crime. There were numerous active or past cases, in particular "revenge porn" or objective material being posted on social media. There is a lack of local capability in many countries to assist with these cases. The impact of these crimes can be extreme, including anecdotal stories of suicide, emigration and severe social/reputational harm.
    - Child exploitation / pornography – this may stem from cultural and/or local differences in the commonality of these crimes for participating countries, but is compounded by the growing use of social media (especially Facebook) and the immaturity of local police, parents, teachers and other professionals to combat these crimes. International support in this space is more readily available, but there is a local need for self-service guidance (see New Zealand's Netsafe program) and appropriate legislation to confirm all enforcement and legal avenues are available when it occurs.

Additional cyber risks (especially to critical infrastructure and valuable/sensitive information) will continue to increase as these countries become more connected, collect more information, and invest in infrastructure.

3. **There is a low level of cyber security maturity across the region.**
The majority of the participating countries have low awareness and maturity across Government in regards to cyber security risk. This is likely driven by mixed priorities and a lack of awareness at a senior

Government level, and therefore the lack of an overarching mandate to manage cyber risk. In many countries, this means that there is no strategy or work plan to uplift cyber security, and key roles and institutions have not been established/defined.

We observed that countries with a strategy, institutional leadership, appropriate legislation, and/or a local CERT were typically more mature in managing cyber security risk – but also more aware of the gravity of the work ahead of them to protect their people, information, finances and critical systems. Broadly speaking, we found the understanding of cyber security risk was stronger at the operational levels, and there would be benefits to providing fit-for-purpose briefing information to senior Government (macro) and key ministers (specific risk to their portfolio) as a part of uplifting governance.

There are strong pre-existing relationships between countries in the region, as each country faces similar challenges. As such, there is value in executing regional initiatives – especially when they deliver value and opportunities on a country-level. There are a number of region-wide cyber initiatives that have been effective and seen as valuable. These include:

- The Australian Cyber Cooperation Program – a major programme of work funded by the Australian Department of Internal Affairs (with support from the New Zealand Government). This initiative focused on establishing international frameworks, cyber crime prevention and legislation, cyber incident response, freedom of online speech and technology good practice. It is supported by more than AUD$34m in funding out to 2023.
- The Pacific Cyber Security Operational Network (PaCSON) - established on 30 April 2018, as a network of government-designated cyber security incident response officials from across the Pacific. This is funded out of Australia's Cyber Cooperation Program and has been well received with operational cyber security professionals in the region.
    - There is a desire to see this initiative expanded to include hands-on training, MOUs for information sharing and more – see our Pacific Cyber Regional Hub recommendation.
- The Cyber Safety Pasifika Program – which has involved cyber training for police, teachers and students). The focus of this program is to help young people stay safe online. It is also funded by DFAT in Australia and supported by the Australian Federal Police.
- The Pacific Islands Law Officers' Network (PILON) Cyber crime Working Group – which has helped to build awareness and skills sharing for the legal, police/enforcement and judiciary. In particular, they hosted a conference in Tonga (including the majority of Pacific Island countries relevant to this report) with a cyber crime focus in 2018.
- The Council of Europe and Australian Attorney-General's Office have both provided assistance to a number of participating countries in legislative drafting for cyber crime, and in some cases provided more broad assistance with advice, training and strategy support in regards to cyber crime.

There have also been unsuccessful projects and programs, including the now closed Pacific Cyber Emergency Response Team (PacCERT). We address factors that limit the success of projects in our next key insight below.

We also noted that many participating countries have been successful in leveraging the assistance of countries outside of the region with initiatives to help increase cyber resilience in the region. Some highlights include:

- Law enforcement from the US, Australia and New Zealand. The relationship with the FBI for the US-aligned Pacific countries has been especially effective to recover money from cyber-crime and fraud. Australia (and to a lesser extent New Zealand Police) have also been very active in building capacity, particularly in the South Pacific.
- The development of local CERTs e.g. AusCERT has been engaged to assist with the development of a Samoa CERT, and the new PaCSON initiative is being chaired by CERT NZ.
- The development of cyber crime legislation, in particular the Australian Attorney-General's Department, NZ Parliamentary Counsel Office and Council of Europe have supported legislative drafting for the development of cyber crime legislation in several Pacific jurisdictions.

4. **Any initiatives in the region should be linked up with existing workstreams, and focus on local ownership, bilateral opportunities and building local capability.**
   a. *Take advantage of existing forums and initiatives, as opposed to creating overlaps with new initiatives.*
      There are a large number of regional forums and groups supporting various initiatives and regional priorities. We found that some were well known and attended (i.e. PaCSON, PILON and Cyber Safety Pasifika), while many others were only known by a limited number of people. The large number of forums can create fatigue and confusion with participating countries, and so new initiatives should deliberately focus on bolster or linking to existing forums (even consolidating them).

   b. *Focus on bilateral opportunities that enable governments in the region to share technology, resources and templates*
      While there are a number of opportunities for regional activities, there are also specific country-level needs that would benefit from a bilateral or multi-government approach (including consider previous projects and whether a similar approach would be beneficial). Many countries across the region showed ease and willingness in regards to working with other Pacific partners, and a joined up approach could reduce costs and reliance on international support. For example, using the same technology solutions and/or templates in multiple countries will enable the sharing of knowledge and skills without needing specific international vendor support.

   c. *Local ownership, skills development, documentation and operational funding are critical to long-term success.*
      Initiatives are significantly more effective in the medium term is they build local ownership and skills. An example of this is Cyber Safety Pasifika, where the AFP train local police officers and teachers to be able to teach basic cyber hygiene and safety tips with local students and communities, as opposed to traveling to these communities themselves. In contrast, PacCERT was largely removed from participating countries (aside from updates) and local value was limited, therefore they were not prepared to fund it. In addition, we observed a number of projects where systems were no longer supported due to a lack of local skills and documentation. All projects executed by international donors should have local ownership/involvement, and sustainability through operational funding as a key requirement.

   d. *Secondment and hands-on training are significantly more valuable than shorter (circa 1-5 day) classroom sessions.*
      While a number of cyber security training options exist through various channels (there is also an opportunity to consolidate per our recommendations), these training sessions are often aimed at an audience with broad maturity and are generally covering only surface elements. There is a strong local desire for real international/local secondment opportunities which create hands-on skills that can be bought home.

   e. *Procurement of technology should be linked up across countries (to share skills), include cyber security requirements and should be driven by local needs.*
      Many Pacific Islands countries will find it easier to access skills from another regional partner than from an international contractor. In cases where systems are effective locally in participating countries, there is a desire from other countries to use those systems instead of building something new. In practice, Pacific stakeholders consistently told us that technology procurement was largely driven by donor agencies (or their consultants) who would sometimes select a product they knew, as opposed to a product that was the right local fit. There is an opportunity (see our recommendations) to consider more centralised procurement and involve local experts in the design/select phase.

      In addition, a number of technology projects (ranging from local databases/systems to industrial control systems for power) do not appear to include appropriate security requirements. Based on a

lack of local capability, it will be critical to include appropriate security controls within the design and build phase of these projects, as it is unlikely (and more costly) to be addressed at a later date.

f. *Consider, but do not be limited by regional alignment and context.*
Culturally, each participating country has a very different local context. Therefore, any proposed initiative in the Pacific region should consider these differing local contexts and how best to optimise implementation for the region. These should not be seen as a reason not to execute regional initiatives, but rather consideration should be given to balancing "one-size-fits-all" templates and guidance, and to providing training and consulting to each country individually (even in a group setting).

Furthermore, for cyber incident response and other ongoing partnerships, we recommend considering alignment (based on history and geographical location):

US Aligned

Marshall Islands, Palau and Federated States of Micronesia

Have laws and partnerships that align with US, including support from entities such as the FBI.

Australia / NZ aligned

Samoa, Tonga, Cook Islands, Niue, Tuvalu, Kiribati, Nauru, Vanuatu, PNG, Solomon Islands and Fiji

Collaborates well with, in particular: DFAT, MFAT, CERT NZ, AusCERT, Australian Federal Police and NZ Police

Policy and Legal Gap Analysis

Executive Summary

Key regional insights

TIMING

The Pacific region is exposed to the cyber threats that the rest of the world is grappling with - from cyber bullying and card skimming to phishing and false invoices to child pornography. This has not only caused financial losses running to millions of dollars, presenting a very real threat to financial systems in the region, but also a risk of harming the physical and mental wellbeing of the region's citizens.

The risk footprint will become larger as Pacific countries increase their online connectivity through improved infrastructure, increased uptake of social media, improved ICT literacy and increased availability of, and reliance on, e-services. Now is the time for governments to take measures to address cybersecurity issues effectively, such as through greater awareness, capacity building and improved legal and regulatory frameworks.

Deloitte has identified 14 key types of cyber risks that the Pacific region currently faces across 4 harm areas:

Economic	Facilitation of international money laundering and funding of terrorism	Financial harm due to fraud or unauthorised access to banking	Inability to process or receive international payments	Inability to meet international standards for e-transactions (i.e. PCI)	
Safety and Wellbeing	Facilitation of the creation, transmission or sale of objectionable or pirated material (i.e. child exploitation)	Harm to individuals due to identity theft, cyber bullying or blackmail			
Disruption	Business disruption and/or impact to wellbeing due to critical infrastructure outage	Inability to facilitate secure and reliable communications channel for international relations/business	Destruction or ransom of information	Malicious altering or defacement of Government information	Interruption to logistics/travel
Trust and Reputation	Facilitation of global cyber attacks originating from the Pacific	Theft of intellectual property, personal information or sensitive data	Driving a malicious political agenda through hacktivism or social media.		

These localised risks can have global consequences, creating a global responsibility to have appropriate cybersecurity, vigilance and resilience in the region.

We note that some countries in the Pacific have relatively limited connectivity and low and/or scattered populations, and lower value at risk compared to global targets. Those practical constraints mean cyber risks are currently somewhat nascent. However with limited awareness and reporting also, it is hard to be definitive about the current level of activity. Our in-country consultations identified that in more developed Pacific countries like Vanuatu, Samoa and Tonga, cyber risks have come to pass.

Looking forward, the continuing drive to connect the Pacific by submarine cable and satellite means that all Pacific countries will be increasingly vulnerable to these risks. The expected increase in online shopping / transactions and payments, use of social media, and digital control systems for important infrastructure, are also relevant. The time for Governments to take action is now. The purpose of this report is to help prioritise attention and funding to those areas which will make the most difference in raising the standard in all Pacific countries on cyber issues.

IMPORTANCE OF FRAMEWORKS

There is the opportunity for the Pacific to make a good amount of progress in a relatively short period of time.

In our discussions Pacific stakeholders regularly emphasised the importance of getting legal and regulatory frameworks in place, as a way of guiding policy focus and capacity building. While in the cybersecurity area a lot of Pacific countries are starting from a low base, the fundamental building blocks that are needed are well known, and highlighted in this report. The task for each jurisdiction over the next couple of years is to get the fundamental building blocks in place.

Some Pacific countries have developed cybersecurity strategy documents (for example, Papua New Guinea, Samoa and Vanuatu). These are valuable as they establish a common picture for the public and private sector in each country about the priority actions on cybersecurity over the next couple of years. All of the Pacific stakeholders we spoke to supported the view that each country would benefit from a strategy document that captures the national story on cybersecurity.

Other big gains to be made include:

- Each country clearly establishing how it will manage cybersecurity for critical infrastructure and systems (including government information systems);
- A number of Pacific countries have enacted criminal law legislation for cyber-crime offences modelled on the Budapest Convention, or are in the process of upgrading existing law to this standard. Pacific countries can continue this effort, and learn from experiences to date as they do so;
- This legislative progress can and should be supported by a focus on building the capacity for effective investigation, enforcement, prosecution and adjudication of offences. Across most of the Pacific, building the front-line capacity for responding to cybercrime is a major opportunity for improving cyber-security.
- We particularly want to emphasise how this investment in effective investigation, enforcement, prosecution and adjudication can address the risks of cyber bullying and [child exploitation]. These issues were stressed to us during consultations as being current and serious risks, with consequences for individuals and communities.

As well as these frameworks, our gaps analysis, risk assessment, and discussions with Pacific stakeholders to date indicate that Pacific governments can improve the management or mitigation of cybersecurity risks by investing in:

- capacity (regulatory, enforcement, technical);
- public awareness of the size, scope and scale of risk, and the roles that all individuals can play in reducing these risks;
- a consistent regional approach to identifying, reporting and sharing information on cyber risks, cyber incidents, and practical mitigations across the region.

OPPORTUNITY TO ADDRESS RISKS AT REGIONAL LEVEL

In our view, we see the key regional opportunities as being:

- implementing cybersecurity and digital strategy in the region and developing a consistent approach to coordinating strategy across the Pacific, where interconnectedness requires a coordinated and consistent approach;
- preparing a legal framework which sets out key functions and responsibilities of cyber stakeholders, deals with cybercrime, and allocates funding;
- building capacity at a regulatory, enforcement and technical level and identifying a clear strategy or funding to develop regional resource and capacity;
- improving cybersecurity safeguards for critical infrastructure; and
- increasing public awareness of cybersecurity and digital issues.

In these areas there is the opportunity for governments and development partners to aim for consistency of approach and implementation across the region. This will help with the development of common knowledge and expertise across the Pacific, as well as promote efficiencies in implementation.

Our recommendations address each of these opportunities for improvement.

Regional Recommendations

Although the countries considered in this study are in varying states of legislative and regulatory development for cybersecurity and electronic transactions, we have identified a number of consistent trends across the Pacific region. These trends enable us to make the following recommendations for regional-level development.

We have also recommended a prioritisation of effort. While all of the proposals discussed in this report will improve circumstances in the Pacific, they cannot all be done at once.

An effective reform can involve building the understanding and demand for change, introducing quality and appropriate legal frameworks, and, most importantly, investing over several years in the institutions charged with implementation. Done well, each reform will involve a lot of effort. Pacific jurisdictions, like all jurisdictions, must prioritise their efforts.

When thinking about prioritisation in this area, Governments and development partners will weigh up the scale and capacity of existing institutions in-country, the capacity for reform and implementation of new laws and enforcement of those laws, the current state of progress in-country on cybersecurity, and the current level of online commercial activity and whether supporting legislation is needed at this stage.

It is important, too, to bear in mind that scale varies significantly across the Pacific. Using population as a rough estimate of scale, the variation in scale across this study is as follows:

Country	Population
Papua New Guinea	8,418,300
Fiji	912,241
Solomon Islands	623,300
Vanuatu	282,100
Samoa	197,700
Kiribati	118,400
Kingdom of Tonga	109,000
Federated States of Micronesia	106,200
Republic of the Marshall Islands	53,100
Palau	22,000
Cook Islands	17,400
Nauru	11,300
Tuvalu	11,300
Niue	1,600

We consider some urgency should be attached to implementing, in a way appropriate for local scale and circumstances, recommendations 1 to 5 below (priority I recommendations). As a generalisation, and depending on the circumstances in each country, the cybersecurity building blocks should be prioritised over the commercial law frameworks. At a basic level, developing cybersecurity strategies, capacity and awareness building and safeguarding critical infrastructure across the region are high priority needs, to ensure Pacific countries are not left vulnerable as the region becomes more connected, digitally focussed and, consequently, a potential target for hackers and fraudulent digital operators. Recommendations 6 to 9 can be considered priority II recommendations. As we identify in the individual country recommendations, some of the larger Pacific countries that are more advanced with their cybersecurity initiatives are better placed, and have more of a need, to give the commercial frameworks some priority.

Priority I recommendations

1 Develop cybersecurity strategies

Coordinated action to address cybersecurity risk at a country level starts with a documented cybersecurity strategy. Countries with a well-prepared strategy or cyber policy include Papua New Guinea, Samoa and Vanuatu. Developing a cybersecurity strategy is an important step to identify and prioritise goals, determine institutional responsibility and allocate resources. A strategy will give impetus and direction to each country's efforts to improve its cybersecurity, especially if each strategy is updated every few years, so that it remains current.

We suggest there is value in developing a model or template cybersecurity strategy for Pacific countries to use as a starting point. Each country can then use the template to document the actions they intend to take to manage cyber risk. Some steps in this direction have already been taken: a close study of national ICT policies across the region was part of the ICB4PAC project, and the CTO prepared a "Commonwealth approach" for developing national cybersecurity strategies in 2015. Drawing this work together to develop an easy-to-use template would assist individual Pacific countries in the process of preparing their own cybersecurity strategies.

At the September 2018 Pacific Islands Forum, leaders endorsed the BOE Declaration on regional security, which expanded the concept of regional security to include, among other concepts, transnational crime and cybersecurity "to maximise protections and opportunities for Pacific infrastructure and peoples in the digital age". This helpfully elevated the profile and priority of cybersecurity in the region.

In response, the Pacific Islands Forum Secretariat has developed a draft action plan for implementation of the BOE Declaration by Pacific countries. Consultations on the draft action plan were held earlier this year. In relation to cybersecurity, the draft action plan proposes:

- promoting and supporting Forum Members accession to the Budapest Convention;
- sharing information on cybersecurity and cybercrime threats and trends;
- supporting the development of national cyber policies and legislation;
- promoting awareness and educating our people on responsible cyber behaviour; and,
- development and strengthening of Computer Emergency Response Team (CERT) capacities (national and regional).

This action plan helpfully maps against some of the priorities that were emphasised to us by Pacific stakeholders during our consultations, and key areas we would hope to see in a national cyber-security strategy.

We also understand that a Cybersecurity Centralised Monitoring initiative is proposed, through PIRRC. We recommend that the initiative include reporting mechanisms and processes to report regularly to identified stakeholders in each country on status and trends in cybersecurity (regionally, and globally), to help inform decision makers in each country when defining and implementing cybersecurity strategies.

2 Cybersecurity awareness

In practice the level of security in the Pacific can be lifted with a concerted effort on awareness, and basic training in cybersecurity hygiene.

Pacific leaders, policy makers, enforcement officers, government officials, financial institutions, infrastructure providers and the general public must understand the nature of the threats online so that they can protect themselves, and take the appropriate action when a threat arises. At the start, raising general awareness could be as simple and as cost effective as a short TV programme.

People regularly use the same email account for personal and work use. And yet individuals do not often receive the benefit of training on how to spot phishing and other cyber hacks that happen at the individual level. A lift in cyber-security hygiene can be the most effective measure in any company, institution or country.

We don't under-estimate the practicalities of rolling out training in the Pacific. Many Pacific countries are spread across a wide geographic area and achieving consistent and broad coverage of cyber awareness programmes can be challenging. There are helpful on-line tools that can be used, and various ways could be used to reach people: schools, the public sector, key infrastructure providers, and so on.

While Programmes like Cyber Safety Pasifika are doing a good job at raising awareness in many Pacific countries. While Cyber Safety Pasifika has been well received, stakeholders also recognised that it relies on the train-the-trainer model (in this case, the Police), which in turn relies on the local trainers having the capability, time and resources to deliver training in-country. Our in-country consultations identified a desire for more broad-based and coordinated awareness building.

Coordinated funding for public awareness building programmes at a regional level, with implementation at a local level, would be a useful regional initiative. A framework awareness building programme could be developed with cultural-specific implementation at a country level. That framework should cover programmes in schools, and community initiatives specifically addressing cyber bullying, child exploitation, as well as a broader programme of digital awareness for online transactions and fraud protection.

We are aware that USP and AFP are currently developing free cybersecurity awareness raising courses to be delivered online and offline. This is a promising development. When it comes to delivery we would encourage a focus on practical delivery channels in each country (for example, in Vanuatu, reminders are texted to all customers on mobile networks) and co-ordination with other efforts in the Pacific.

3 Continue to enact up-to-date cybercrime legislation

There is progress across the Pacific in enacting cybercrime legislation. A number of countries in the Pacific have either enacted cybercrime legislation modelled on the Budapest Convention or have processes underway to develop existing legislation to this standard. It is important that this effort continues, and that countries without modern cybercrime legislation are encouraged to reform their legislation as appropriate.

Many stakeholders we have spoken to confirmed that legislation drives changes in institutional behaviour around cybersecurity. Without legislation as a guideline to action, government agencies and other organisations find it hard to take it upon themselves to address cybersecurity and cybercrime issues. Furthermore, by formalising cybersecurity functions of key government ministries, these ministries should receive the budget support required to implement or enforce cybersecurity and cybercrime measures.

To date there have been a number of prosecutions for cyber-related crimes in the Pacific using local crime and penal code provisions. This has been a useful way to address cyber risks in the short term, but is considered by stakeholders to highlight the genuine need for up to date legislation.

The legislative drafting programmes run by the Australian Attorney-General's Office appear to have been particularly helpful in assisting countries to develop cybercrime legislation. We recommend expanding these programmes and/or funding similar exercises elsewhere, such as in the Northern Pacific. Some key benefits of this programme have been to create connections between different countries, as well as to facilitate thinking around governance, capacity and enforcement issues in-country while legislation is being developed. This programme, or a similar programme, could also create a channel for exchange of legislation drafting, helping countries at different stages of the legislation drafting process where capacity may be lacking or constrained. Alternatively, a model legislation template would assist individual Pacific countries to prepare their own cybercrime legislation. However, this option would still require the assistance of experienced legislative drafters – as enacting cybercrime legislation would require review of a number of existing laws, including laws relating to evidence, police, criminal offences, electronic transactions, consumer protection and financial institutions.

We also recommend that when updating cybercrime legislation, governments put in place enforcement protocols or memoranda of understanding between key enforcement stakeholders, such as the Attorney-General's office, Director of Public Prosecutions, Police, ISPs etc. Our consultations in-country confirm that stakeholders will benefit from having a formal framework to establish cooperation in enforcement, and to provide protocols to be followed by different stakeholders in response to a cybersecurity incident.

4 Capacity-building: law enforcement, prosecution services, law practitioners and the judiciary

A country's ability to enforce a cybercrime legislative framework relies on effective investigation, prosecution and adjudication of cybercrime offences. The effort of passing new laws is only worth it if there is also the follow up commitment to support the people and institutions who will be tasked with implementing the new laws.

In most Pacific countries, improving the capacity for responding to cybercrime is a high priority and a real opportunity to make gains. Significant effort should be devoted to improving this capacity, by providing training on investigating cybercrime and collecting digital evidence, and by ensuring appropriate resources (both human and financial) are allocated to combatting cybercrime. It may be most effective to conduct much of this training at a regional level, utilising instructors available from Australia, New Zealand and the United States.

As noted above, this investment in investigation, prosecution and adjudication capability can address the concerns expressed in the Pacific about better responding to cyber-bullying, child pornography, and the need for greater child protection online.

Capacity building in this context could also include developing a specific process for law enforcement to work with social media platforms, particularly Facebook.

In some of the smaller Pacific countries – particularly those where incidents of cybercrime are rare – it may not be practicable to train and recruit dedicated cybercrime specialists in law enforcement and prosecution services. For this reason, international cooperation links across the Pacific should be strengthened, so that this type of resource is available to low-capacity countries when required.

5 Capacity-building: regional hub

Considering the four priorities identified above, we suggest that a regional hub for cybersecurity would be valuable. This does not need to be grandiose, and it can be focussed on providing practical assistance to Pacific countries looking to put in place these fundamental cyber-security building blocks.

The regional hub could consolidate information, training, projects and services, and contacts, into one place. It could cover the following ground.

Collecting and sharing information:

- provide regional templates for cybersecurity strategies;
- provide regional templates for model legislation;
- provide regional templates for MOUs between enforcement agencies and stakeholders;
- share practical approaches to improving the security of essential infrastructure;
- share information on cybersecurity workshops, meetings, training course, scholarships, secondment opportunities;
- share information on risks that are being identified.

Some very early gains could be made with a simple website that collected and shared information on these key areas.

Centralising incident reporting, and Pacific-wide alerts and warnings.

Provision of services and capability to Pacific countries:

- advanced cyber incident response support for in-country teams;
- technical templates for building secure services (e.g. a template for a secure payments website);
- security and vulnerability testing services;
- centralised procurement for security and IT services;

Capacity building across the Pacific:

- The hub could be the focal point for the provision of targeted capacity building and training in cybersecurity;
- For example, it could arrange for short-term workshops on cybersecurity;
- Secondments could be offered to help local experts upskill.

We are aware that the idea for a cybersecurity centre or facility has been suggested by USP. The suggestion was that USP had already started offering cybersecurity courses and was therefore well placed to continue to provide this in the region. However, in our discussions with some Pacific stakeholders, there were strong views that the hub should not be placed at USP. Current cybersecurity courses being offered at USP were seen to be too academic (with the preference being for shorter training modules with a more practical approach), eligibility requirements too high, courses too expensive, and therefore cost prohibitive. PacCERT was based at USP and it failed to generate sustainable support. In our view, Vanuatu would be a good candidate to establish and build support for a hub. There are good facilities, capable people, and an existing focus on activities and services that are seen to deliver tangible value.

Priority II recommendations

6 Safeguard critical infrastructure and services

Some material gains can be made in the larger Pacific countries in managing cybersecurity risk for critical infrastructure, where digital management systems are in place. Pacific countries should be encouraged to identify operators of essential services dependent on network and/or information systems, and require these operators to take appropriate technical and organisational measures to address security issues. These security measures could be formalised either as recommended guidelines or as legislative requirements, depending on how the relevant piece of infrastructure is owned, and regulated, in the relevant country.

We would expect these measures to consider Prevention (software patching, system-level risk assessment, basic security technology like firewalls and anti-virus software), Vigilance (vulnerability scanning, security monitoring), and Resilience (off-island back-ups, CERT and incident response capability).

We expect similar infrastructure and services will be categorised as essential across the Pacific: energy, water, telecommunications, and internet providers. Some regional coordination of efforts to safeguard this infrastructure, therefore, may well be useful. This coordination could take the form of a standardised checklist for countries to follow when identifying critical infrastructure and standardised security requirements for different industries to meet. Cybersecurity should be one of the agenda items at any regional meeting of critical infrastructure providers and funders.

To the extent that regional funding is made available for security initiatives (whether or not as a consequence of the BOE Declaration), that funding could be prioritised to bring countries up to a basic standard of critical infrastructure cybersecurity.

Where foreign aid or donor funding is used to fund critical infrastructure, we recommend that funding cybersecurity steps be a required component of those projects.

7 ICT capacity-building generally across the region

The desire and need for capacity building in the Pacific is not limited to officials. Beyond law enforcement, prosecution and the judiciary, stakeholders in every country we visited identified a lack of capacity in the ICT area generally as the primary limiting factor in developing better (or any) legislative and regulatory frameworks for cybersecurity and electronic transactions.

These countries are small, often isolated, and are unable to provide remuneration packages and associated benefits that often attract talented people with an interest in cybersecurity and electronic transactions.

We recommend that the donor agencies consider how it might best incentivise and foster talent in cybersecurity and electronic transactions in the Pacific region, and more importantly to ensure that once people are trained, they remain available to assist their respective Pacific Island countries. There is a real desire for a long-term strategy on ICT capacity in the Pacific.

Some ideas for building local capacity include funding scholarships at secondary school or tertiary level, as well as scholarships for short term or extended training. In many of the Pacific Island countries that we visited, there were one or two well trained and experienced individuals, often employed in the private sector. These individuals would benefit from short term cybersecurity training, at a more advanced level. However, the majority of IT personnel placed within Ministries and organisations required, and often requested, basic cybersecurity training.

Another option would be to fund secondments to organisations in Australia, New Zealand or abroad, which would allow IT personnel to be trained in organisations operating in more established legal and regulatory frameworks. Individuals on secondment would benefit from hands on training provided by experts within these organisations and be exposed to actual cybersecurity incidents and responses. Secondments could be made available across the region, or to a grouping of countries with similar strategies and capabilities.

We note that Digicel (operating in Samoa, Tonga, Vanuatu, Fiji, PNG and Nauru) and other ISPs in other countries are investing significantly in personnel and their cybersecurity and digital economy skills. Together with building local and/or regional CERT capability, public/private partnerships may be another way to build capacity effectively in the region.

USP and Christ's University in the Pacific both offer post-graduate cybersecurity courses. While we cannot comment on the quality of the courses, we encourage the development of "home grown" qualifications.

There may be smart ways to take advantage of the networks of talented Pacific islanders working abroad. Networks could facilitate the exchange of information, help with tailoring response to the Pacific, and with identifying and supporting new talent.

We agree with the many stakeholders who emphasised that building local capacity is essential for implementing and developing the recommendations in this report, now and into the future. As cyber threats will continue to become more sophisticated, local capacity building will need to be maintained and keep apace to deal with new threats. There will be no single answer. A Pacific strategy on ICT capacity will need to pull on as many levers as it can.

8 Privacy and data protection

Compared to more developed jurisdictions, Pacific countries tend to have fewer legislative frameworks directed at privacy and data protection regulation. Most countries have constitutional (or similar) recognition of privacy rights, but have yet to enact concrete legislative protections for the collection, use and disclosure of personal information.

However the comparison with developed jurisdictions does not in itself make this a priority. Local businesses do not appear to be collecting large amounts of personal information for marketing purposes, as is the case in other, more developed countries. Popular demand for enhanced privacy legislation is accordingly currently quite limited. That said, the public's expectations in relation to privacy may increase relatively quickly, given the increasing popularity of social media platforms and associated global publicity of privacy issues.

Before prioritising enactment of privacy legislation, it may be worthwhile investing in policy development. Two key areas were highlighted to us. First, supporting awareness-raising campaigns, so that populations in Pacific Island countries become more cognisant of the risk presented to individual privacy by mass data collection. Countries would benefit from a discussion at the local level about what they want and expect from privacy in the digital age, in the context of small Pacific state. Improved awareness should provide a platform for eventual legislative development.

Second, the size of most Pacific countries means that a standalone privacy agency is unrealistic and unnecessary. For that reason we caution against simply replicating the Australian or New Zealand privacy model for the Pacific (as has already been suggested). There is the opportunity to explore a more tailored response. An effective privacy regime requires a body capable of receiving and investigating individual complaints and which otherwise has an educative role. That body doesn't necessarily need to be a standalone body, or require extensive enabling legislation. An effective privacy and data protection function could be built into the remit of any government body which focusses on individuals, such as a department or ministry dealing with consumer issues, or a body which already has an ombudsman-type function.

The design of a privacy body, and set of privacy laws, that is appropriate for the conditions of a Pacific state, is a good design challenge. It could be grappled with at the regional level. A bespoke Pacific privacy framework, including a code and institutional framework, could be developed. As such, while individual countries focus for the next couple of years on the Priority I building blocks for cybersecurity, perhaps this can be a focus for regional development.

9 Electronic transactions

A few Pacific Island countries have enacted direct enabling legislation for electronic transactions, drawing on the UNCITRAL Model Law on Electronic Commerce 1996 and Model Law on Electronic Signatures 2001.

Electronic transactions legislation serves primarily to confirm the legal validity of electronic communications and electronic authentication methods when parties are trading. Where there is currently no problem with the use of electronic transactions when trading, there may be less need for electronic transactions legislation.

This study has not identified any countries where electronic transactions are currently impeded due to issues of validity under domestic law. We recommend countries focus their efforts on the Priority I initiatives discussed above, for the time being.

It is possible that as electronic transactions become more widespread across the Pacific, more countries will proceed to enact this type of legislation. It is also possible that as these technologies and ways of trading become the global norm, the practical need for confirming legislation lessens. We recommend countries keep in mind the possibility of electronics transactions legislation, recognising also that the UNCITRAL model laws provide an accessible template for this type of legislation if and when required.


PRIF


ADB


Australian
Aid


European Union


JICA


NEW ZEALAND
Aid Programme


WORLD BANK GROUP